MAJOR APPLICATION SYSTEM
System Name and ID

I. SYSTEM IDENTIFICATION

I. A. Responsible Organization

U. S. Department of Agriculture
Agricultural Research Service

I. B. System Name/Title

Name:

ID#:

I. C. System Category

Major Application

I. D. System Operational Status

Operational

I. E. General Description/Purpose

Web Page(s)

Level of Public Access

I. F. System Environment and Special Considerations

System Computing Platform

Name and Type of Firewall

I. G. System Interconnection/Information Sharing

I. H. Information Contact(s)

II. SENSITIVITY OF INFORMATION HANDLED

II. A. Applicable Laws or Regulations Affecting the System

Public Law 100-235, Computer Security Act of 1987
OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
OMB Circular A-123, Internal Control Systems
*Privacy Act of 1974, Public Law 93-579 ***(Remove if not applicable)***
Executive Order 13103, Computer Software Policy, October 1, 1998
Presidential Decision Directive 63, Critical Infrastructure Protection
USDA Departmental Regulation (DR) 3140-001, Information Systems Security Policy
USDA DR 3140-002, Internet Security Policy
USDA DR 3230-002, Disposition of Excess ADP Equipment
USDA DR 3300-1, Telecommunications and Internet Services and Use Memorandum Dated March 8, 1999, Interim Department Computer Incident Reporting Procedures
*USDA DR 3450-001, Computer Matching Projects Involving Individual Privacy Data ***(Remove if not applicable)***
USDA Notice 3140-, USDA Firewall Program Policy (FPP)
ARS P&P 253.3
ARS Information Systems Security Program

II. B. General Description of Sensitivity

Confidentiality

Integrity

Availability

III. SYSTEM SECURITY MEASURES

III. A. Risk Assessment and Management

Status:
In Place Date:

Planned Date:

III. B. Review of Security Controls

Status: **In Place and Planned**
In Place Date:
Planned Date:

An independent management review of the security needs and in-placed and planned security controls for this system was conducted by a consultant firm, “Security for Information Technology, Ltd.” in ________, 2000. The management review included ensuring that the system security plan was prepared in the standard ARS security plan format, that the plan contained adequate and appropriate information about the mission requirements of the system, the technical system components, the protection requirements for confidentiality, integrity and availability and the controls in place and planned for the system and its compliance with Federal, USDA and ARS Laws, Regulations and policies. Based on this management review a detailed report containing recommendations for additional information and other security plan changes and improvements in actual system controls was provided to the System Owner and ARS Management. This review was consistent with the requirements of OMB A-130, Appendix III for independent management reviews.

These types of reviews are performed by organizations independent of the system owner. Although, A-130, Appendix III requires an independent review every three years, it is outside the area of responsibility and control of this system management and a planned date cannot be estimated at this time for a follow-on review.

III. C. Applicable Guidance

USDA Departmental Manual (DM) 3140-1.1 through 1.8, ADP Security Manual
USDA Agency Information Security Policy Compliance Self–Assessment Tool, Guidelines and Checklist
Critical Infrastructure Assurance Office, Practices for Securing Critical Information Assets, January 2000

III. D. Rules

Status:
Planned Date:

III.E. SECURITY CONTROL MEASURES

III.E.1. Management Controls

III.E.1.a. Assignment of Security Responsibility

Status:
Planned Date:

III.E.1.b. Personnel Security

Status:
Planned Date:

III.E.2. Development/Implementation Controls

III.E.2.a. Authorize Processing

Certification:
Status:
In Place Date:
Planned Date:

Certifying Official

Accreditation:
Status:
In Place Date:
Planned Date:

Accrediting Official:

III.E.2.b. Security Specifications

Status:
Planned Date:

III.E.2.c. Design Review and Testing

Status:
Planned Date:

III.E.3. OPERATIONAL CONTROLS

III.E.3.a. Physical and Environmental Protection

Status:
Planned Date:

III.E.3.b. Production, Input/Output Controls

Status:
Planned Date:

III.E.3.c. Contingency Planning

Status:
Planned Date:

III.E.3.d. Audit and Variance Detection

Status:
Planned Date:

III.E.3.e. Application Software Maintenance Controls

Status:
Planned Date:

III.E.3.f. Documentation

Status:
Planned Date:

III.E.4. SECURITY AWARENESS AND TRAINING

III.E.4.a. Security Awareness and Training Measures

Status:
Planned Date:

III.E.5. TECHNICAL CONTROLS

III.E.5.a. User Identification and Authentication

Status:
Planned Date:

III.E.5.b. Authorization/Access Controls

Status:
Planned Date:

Logical Access Controls

Dial -In Access

Wide Area Networks

Screen Warning Banners

III.E.5.c. Public Access Control

Status:
Planned Date:

III.E.5.d. Data Integrity/Validation Controls

Status:
Planned Date:

Malicious Programs/Virus Protection

Message Authentication

Integrity Verification

Reconciliation

Digital Signatures

III.E.5.d. Audit Trail Mechanisms

Status:
Planned Date:

III.E.5.e. Confidentiality Controls

Status:
Planned Date:

III.E.5.f. Incident Response Capability

Status:
Planned Date:

III.E.6. Complementary Controls Provided By Support Systems

IV. ADDITIONAL COMMENTS